



Managed Extended Detection and Response (XDR)

Let US Signal's security experts monitor, detect, and respond to security issues across your extended environment with Managed Extended Detection and Response (XDR). The fully managed security solution gathers data across your entire digital estate to analyze for suspicious activities. The service leverages a third-party software platform to monitor, collect, and correlate data from disparate sources to identify threats and their origination.

US Signal's Security Operations Center (SOC) team receives and responds to all security alerts, freeing up your internal resources and enabling you to leverage the extensive security experience and expertise of the US Signal SOC.

TECHNICAL OVERVIEW

US Signal's SOC team works with your team to manage the deployment and setup of Managed XDR. The service uses a cloud-based deployment model to monitor deployed agents, collect logs, and analyze data with minimal impact on system performance.

Software agents conduct endpoint monitoring and collect data—such as processes, connections, volume of activity, and data transfers—into a central database. Logs and telemetry data are also collected from network devices, cloud services, and more for comprehensive network threat protection.

The solution correlates and analyzes the data to create threat alerts to be investigated by the US Signal SOC. The SOC investigates breaches to determine how an exploit penetrated security and to hunt for remaining threats in the network.

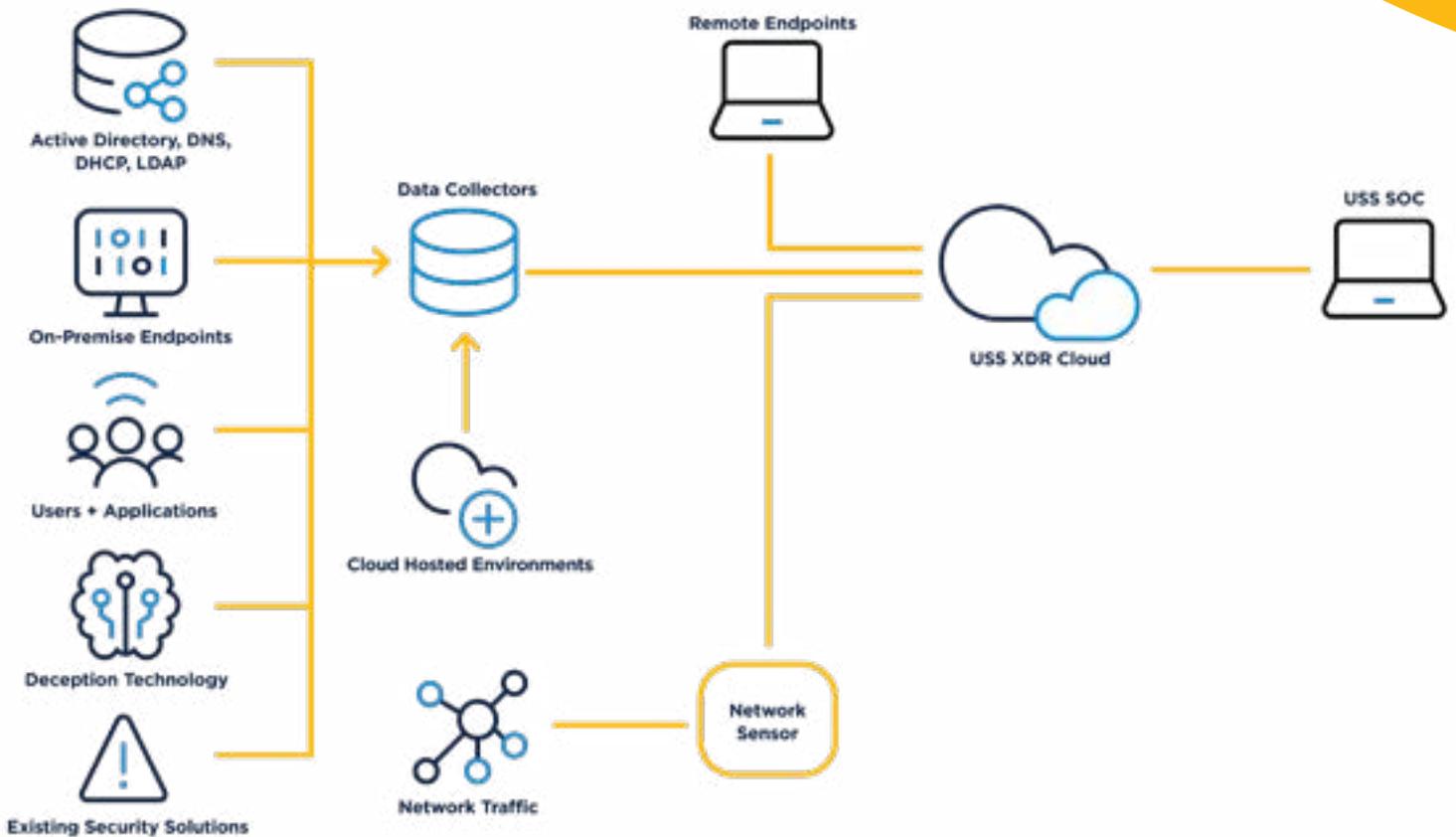
KEY FEATURES

- + Real-time continuous monitoring and collection of data
- + Correlation of data across resources
- + AI behavioral-based detection
- + Cloud-based deployment model
- + Lightweight agents and log collection

AT-A-GLANCE

- + Fully managed 24/7 threat monitoring and detection
- + Monitors and collects activity data from workstations and servers that could indicate a threat
- + Extends monitoring to include network and cloud sources
- + Analyzes and correlates collected data for holistic detection of threat patterns and sources across the entire environment
- + Researches identified threats and search for suspicious activities with forensic and analysis tools
- + Remediation guidance provided by US Signal SOC
- + Vulnerability Management as a Service is available as an add on to your network to provide remediation guidance for identified potential threats

XDR Architectural Design



SERVICE LEVEL AGREEMENT

The response SLA for technical support is one hour from the time a support request is received, during normal business hours, Monday-Friday 8:00 am-5:00 pm ET, excluding holidays. A request is considered received when made to the US Signal Technical Operations Center (TOC), and a ticket is created.

For Managed XDR customers, the response SLA is one hour for customer alert notifications from the receipt of alert within US Signal's Alert Management System. US Signal will use commercially reasonable efforts to notify customers of any scheduled maintenance that may affect the availability of the services.

SERVICEABILITY

Managed Extended Detection and Response (XDR) is available on an annual term basis with a minimum of a one-year term agreement. It can be bundled with other US Signal services or purchased independently.

PRICING

Pricing is comprised of a monthly fee per endpoint, as well as a non-recurring implementation and setup charge. The customer may add or remove endpoints throughout the billing period but will be billed for the highest number of agents deployed at one time throughout the billing period.

SUPPORTED SOURCES

✓ AWS	✓ LDAP
✓ Google	✓ Firewalls
✓ Microsoft Azure	✓ SIEMs
✓ Microsoft 365	✓ Antivirus
✓ Salesforce	✓ Honeypots
✓ Duo Security	✓ Web Proxies
✓ Active Directory	✓ Third Party Alerts
✓ Exchange	✓ DHCP
✓ DNS	✓ Workstations
✓ Servers	✓ Switches

RESPONSIBILITIES

DEPLOYMENT

US Signal provides virtual guidance during the deployment process to ensure proper deployment is achieved. However, the customer is responsible for the execution of the deployment. US Signal can offer physical assistance for deployment if desired, but this will entail an additional cost.

ALERTS & RESPONSE

Alerts will be sent to the US Signal SOC, which will handle the response measures and notify the customer accordingly.

TECHNICAL SUPPORT

Full technical support of US Signal's Managed XDR and the collected data is provided by US Signal. Incident investigation includes review of collected information and analysis within the XDR platform. Any support that requires escalation will be coordinated by US Signal with the customer.

QUOTE

Term:

Order Type:

Quantity:

Per Unit:

MRC:

Total MRC: